Abstract of the Disclosure

A method and a device are ~~proposed~~ disclosed for the low-cost implementation even of high-performance encryption functions in an ~~encryptor~~ composed merely of PC software or the like, or of any other terminal/ information system with integrated Vernam cipher which does not need to be supported by expensive crypto-hardware for the actual encryption process. The crypto-hardware is made either of a chipcard or a multifunctional PC interface adapter (PCMCIA module) with built-in special crypto-hardware. The encryptor, on the other hand, is a conventional personal computer ~~(PC)~~, software or another terminal which, however, with the exception of the very simple Vernam cipher (~~such as~~ EXOR), needs no further crypto-technology even for broad-band applications in software. The external crypto-modules contain all the complex crypto-functions which generate the Vernam key ~~(KV)~~ in reserve, the reserves being temporarily stored in an intermediate storage until they are gradually used up by the encryption process through logic operations of the method. The storage may be installed either in the PC or terminal, or also in the crypto-module. The encryptor always operates with the same Vernam cipher, even if the external crypto- or PCMCIA modules use different symmetrical and asymmetrical ciphers. External crypto-modules in the form of chipcards or PCMCIA modules are inexpensive to manufacture. All the complex crypto-functions are located outside of the encryptor. They are interchangeable by module and can be implemented in the proposed low-cost and somewhat lower-speed external crypto-modules.